

A Resilient and Trusted Internet: Avoiding Fragmentation

For IABOpen of IETF 125

Xing Li

xing@cernet.edu.cn

Tsinghua University

2026-03-18

CERNET, CERNET2, CERNET3



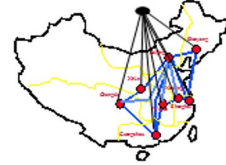
1994

2.4 Kbps - 9.6 Kbps
IP over X.25



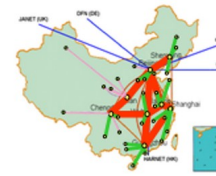
1995

64 Kbps
IP over lease line



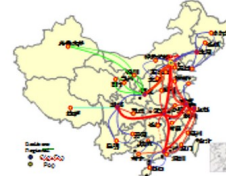
1997

512 Kbps - 4 Mbps
IP over VSAT



2000

155 Mbps
IP over SDH



2004

2.5 Gbps - 10 Gbps
IP over DWDM



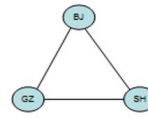
2014

100 Gbps
IP over DWDM



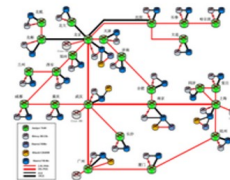
1997

2.4 Kbps - 9.6 Kbps
IPv6 over IPv4



2003

2.5 Gbps
IPv6 over SDH



2006

2.5 Gbps - 10 Gbps
IPv6 over DWDM



2020

100 Gbps
IPv6 over DWDM



100 Gbps
IPv6 slicing over DWDM

Resilient

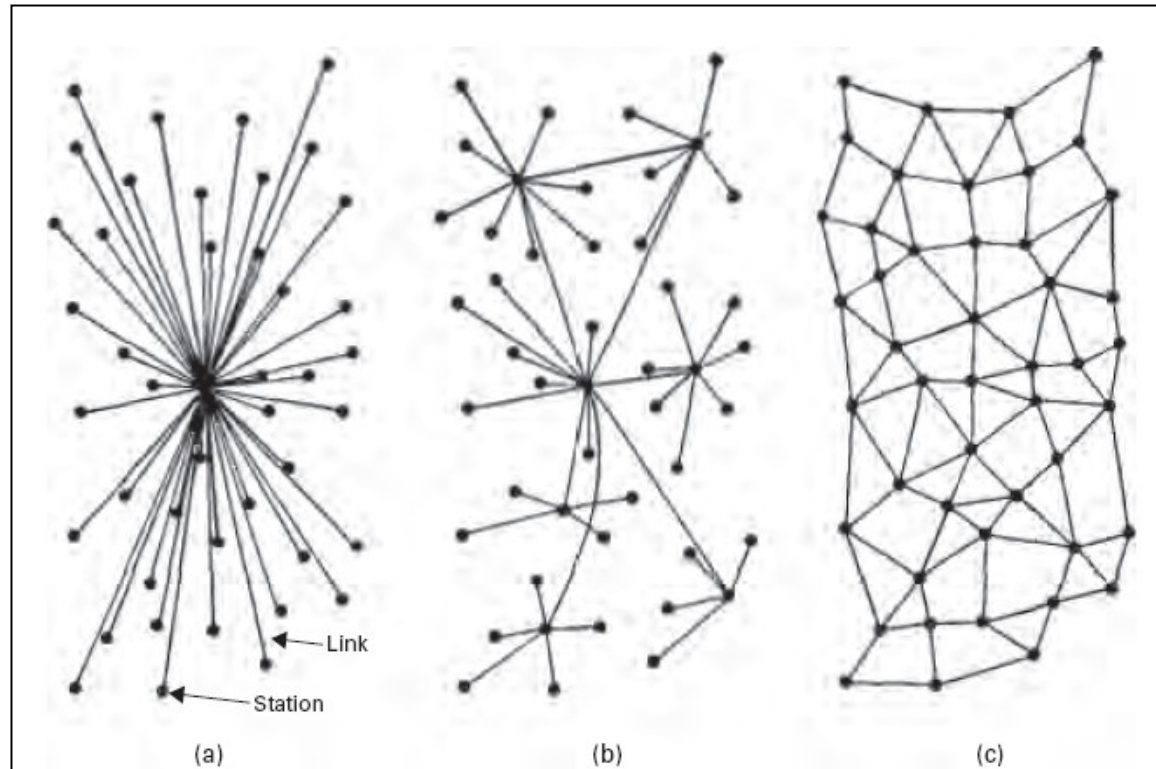
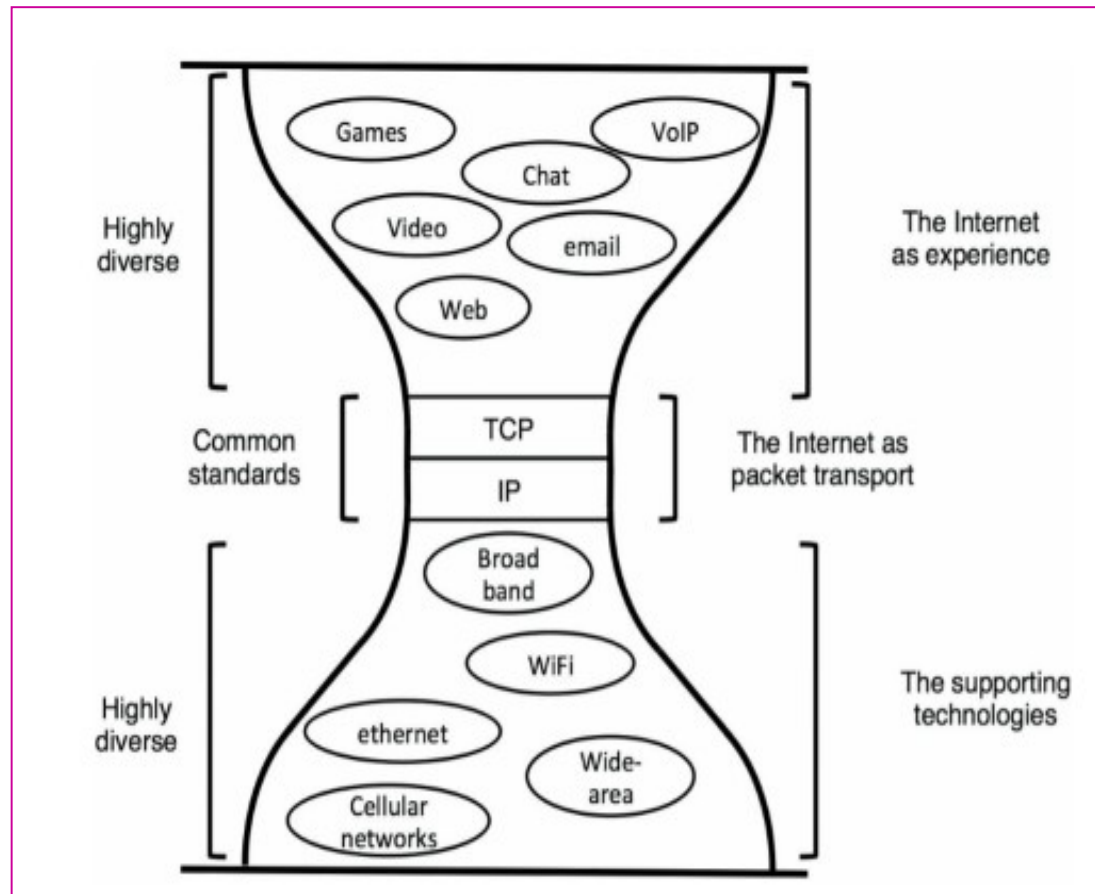


Figure 3.2

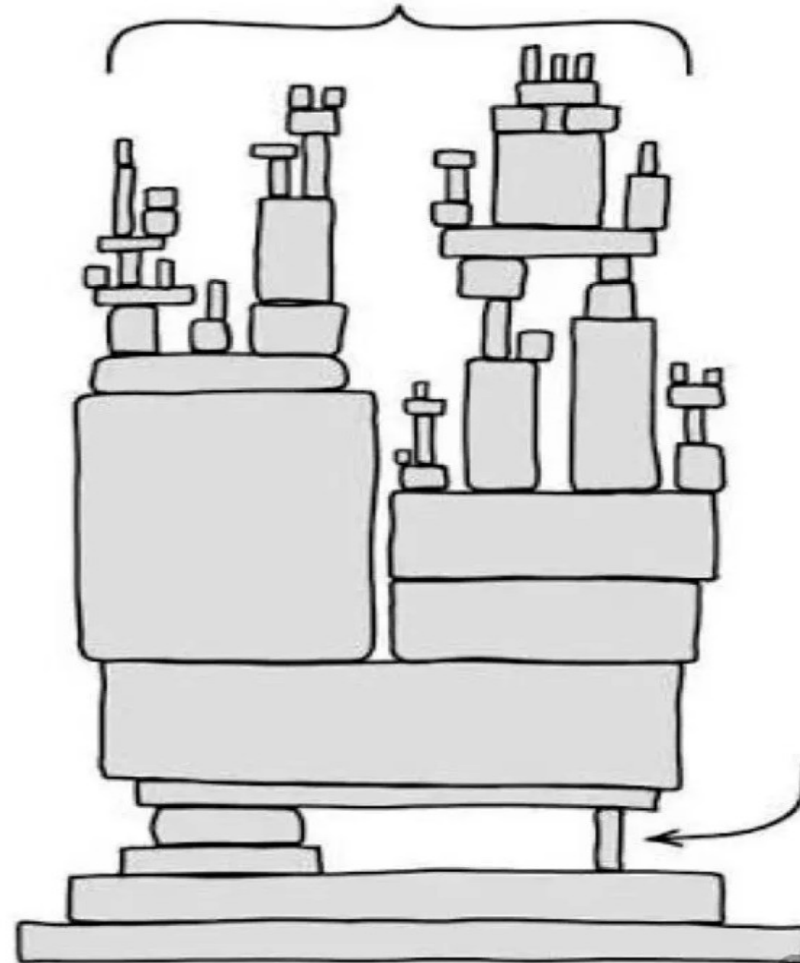
Three network types: (a) Centralized, (b) decentralized, and (c) distributed. *Source:* From Paul Baran, "Introduction to Distributed Communication Networks." *On Distributed Communications*, RAND Corporation Memorandum RM-3420-PR, August 1964, 2. Reproduced with permission of The Rand Corp.

Internet architecture



- Connectionless
- Best effort
- End to end

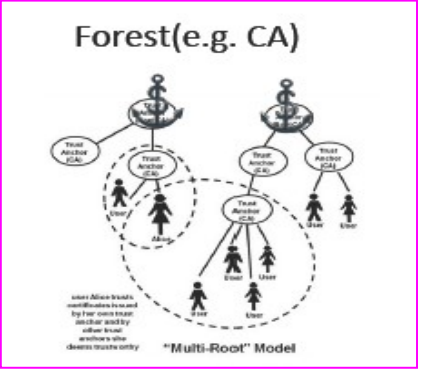
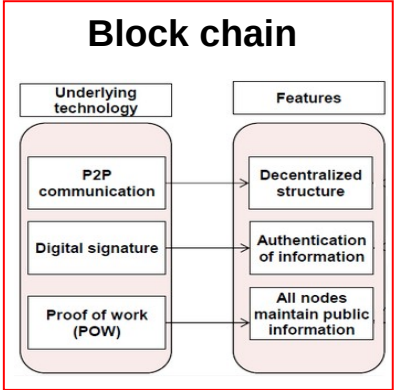
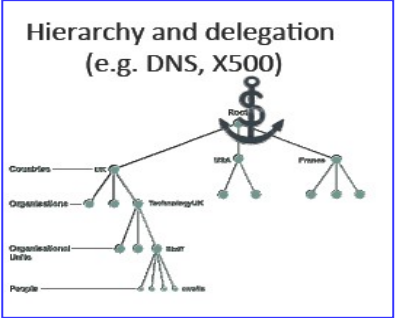
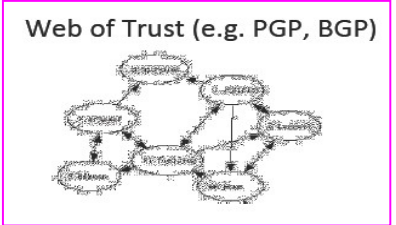
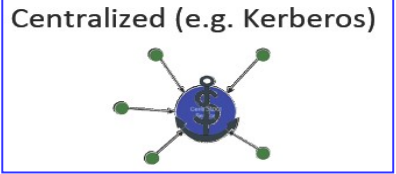
The public Internet



Resilience killer

Trusted model

Trust on First Use,
e.g. SSH, DNS/Cert
Pinning

DNS
DNSSEC
RPKI

TLS

Internet Fragmentation

- **Technical Fragmentation**

- Addressing
 - o IPv4
 - o IPv6
- DNS
 - o gTLD
 - o Hijack
- Security
 - o Firewall
 - o CDN
 - o VPN

- **Governmental Fragmentation**

- Censorship
- Data Localization
- Cybersovereignty
- Privacy

- **Commercial Fragmentation**

- Network Neutrality
- Walled Gardens
- Geo-Localization and Geo-Blocking
- Intellectual Property

- **AI Fragmentation**

- GPU
- Data bias
- Regulations

(IGF white paper, etc)

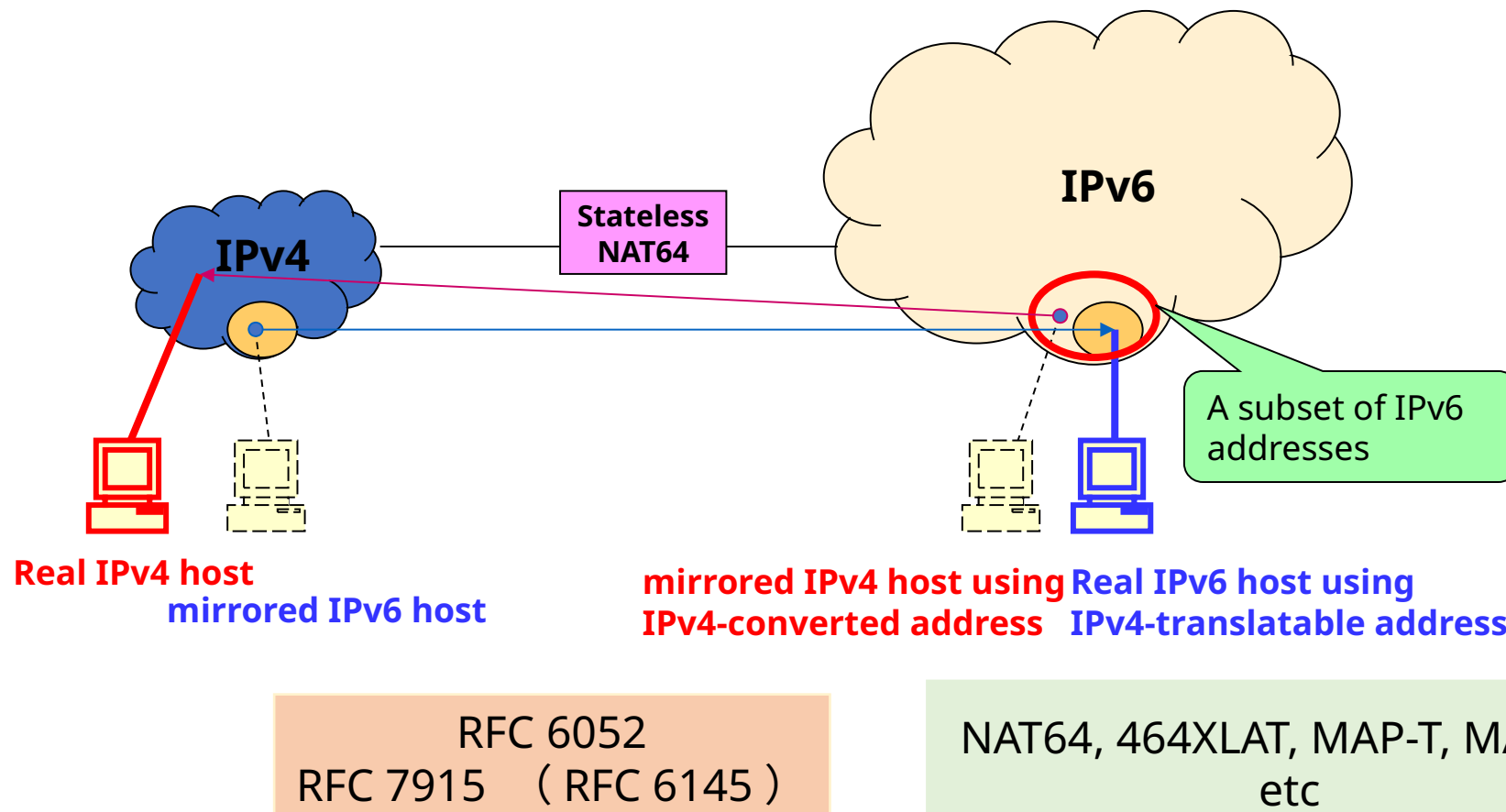
Snowden event (2013)

- The IETF is willing to respond to the pervasive surveillance attack?
 - **Overwhelming YES. Silence for NO.**
- Pervasive surveillance is an attack, and the IETF needs to adjust our threat model to consider it when developing standards track specifications.
 - **Very strong YES. Silence for NO**
- The IETF should include encryption, even outside authentication, where practical.
 - **Strong YES. Silence for NO**
- The IETF should strive for end-to-end encryption, even when there are middleboxes in the path.
 - **Mixed response, but more YES than NO.**
- Many insecure protocols are used in the Internet today, and the IETF should create a secure alternative for the popular ones.
 - **Mostly YES, but some NO.**

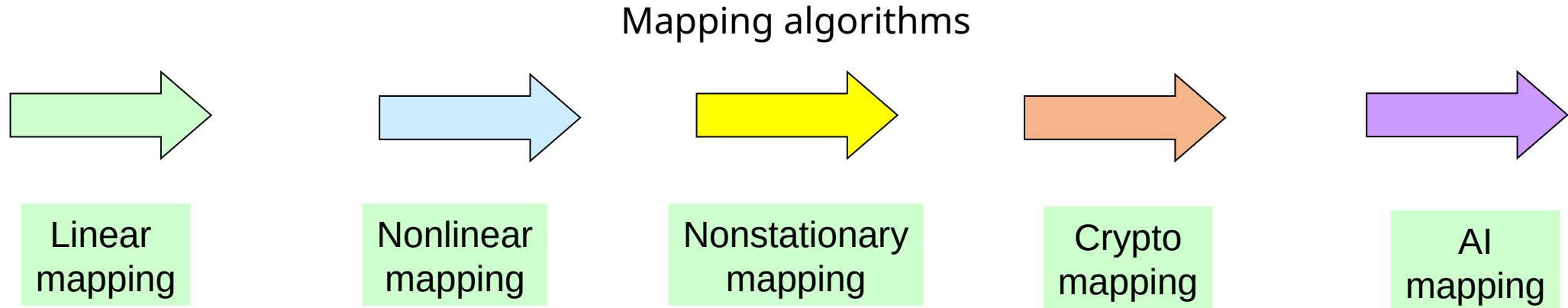


[Hardening The Internet](#)

IPv4/IPv6 translation



6Former (2021)



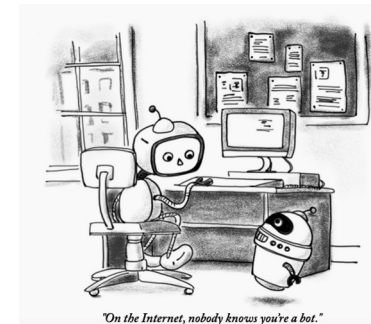
RFC605
2

6Former: Transformer-Based IPv6 Address
Generation

1st Qiankun Liu
Institute for Network Sciences and Cyberspace
Tsinghua University
Beijing, China
lqk20@mails.tsinghua.edu.cn

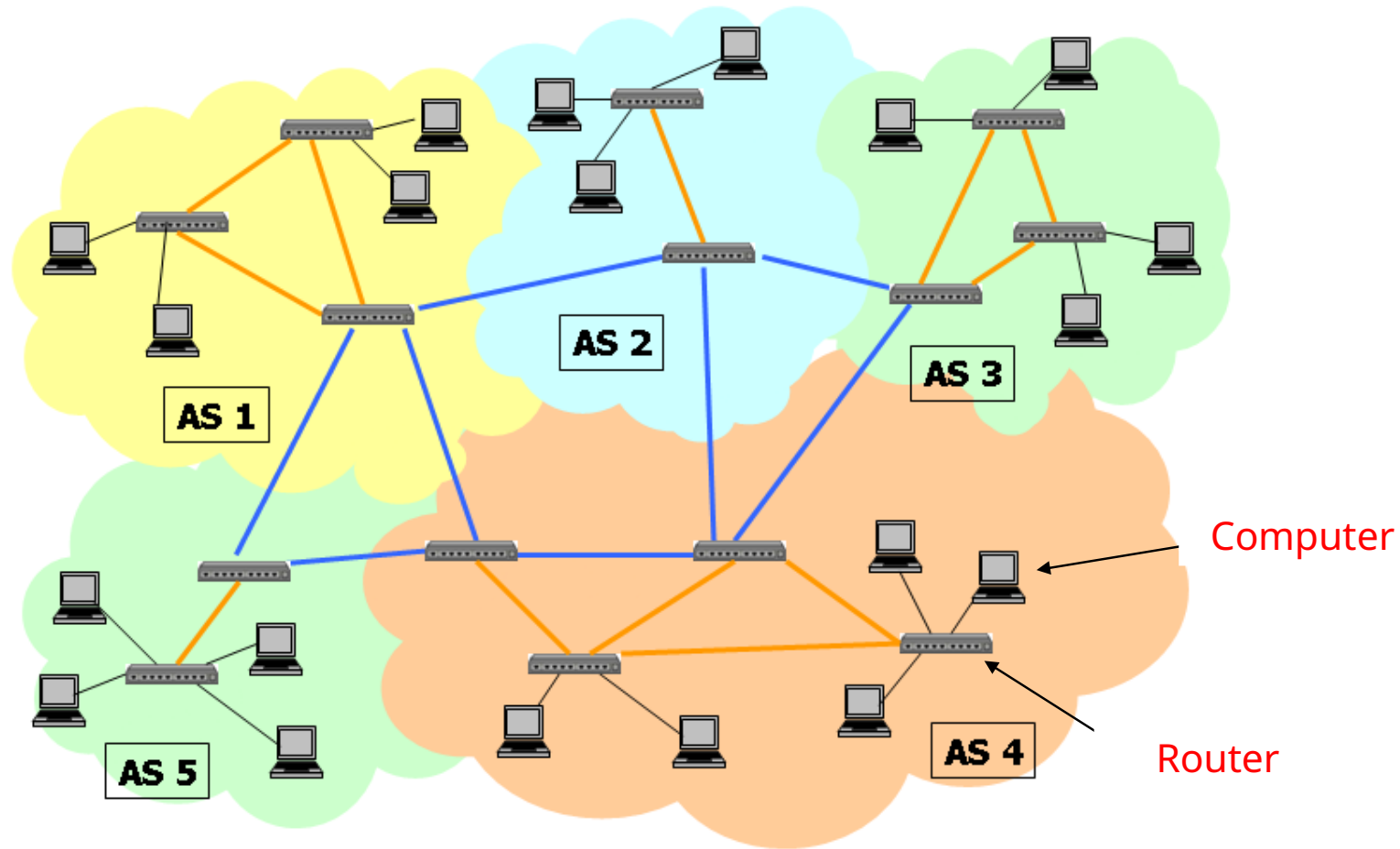
AI Challenges

- Network performance
 - Training
 - Inference
- Fragmentation
 - Geo-localization
- Centralization
 - AI giants
- Trust
 - AI agents



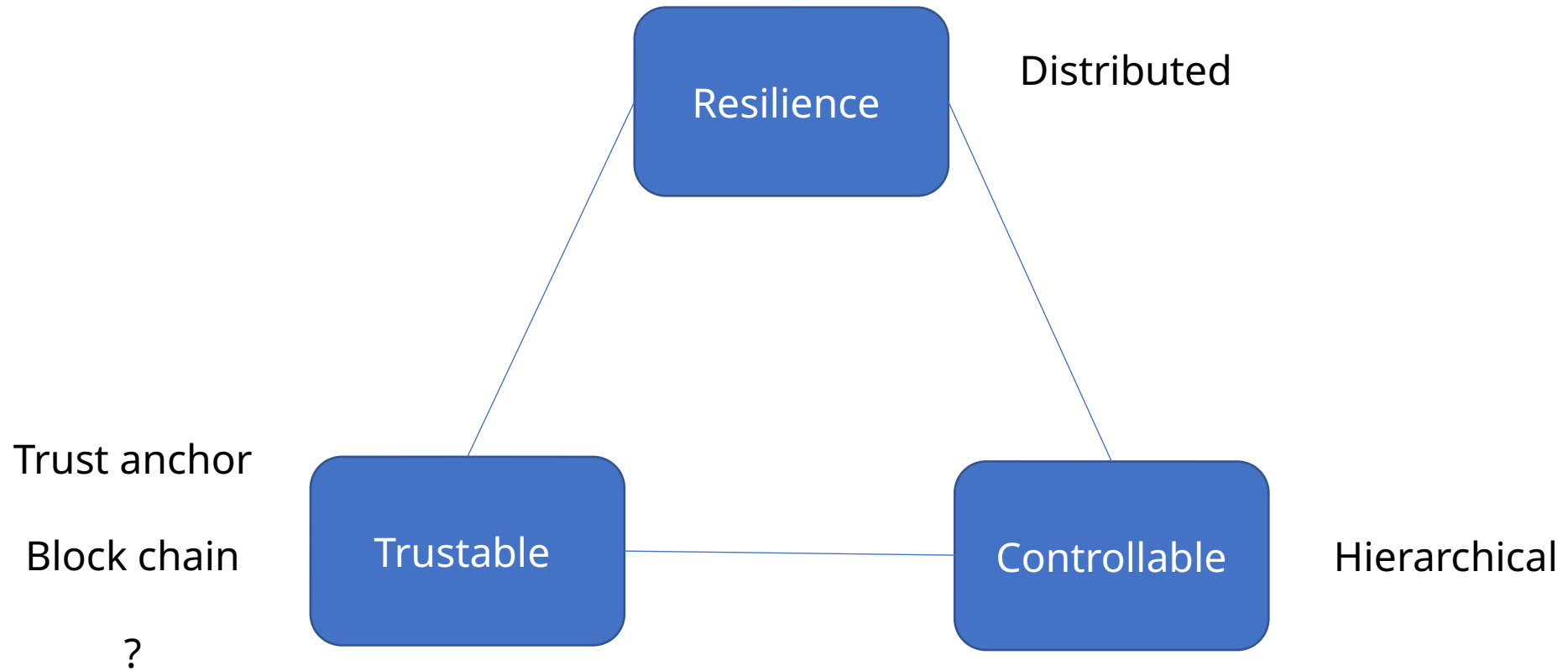
- **AI agents** are servers, not clients
 - Server needs public address
 - IPv4: no way (2^{32})
 - IPv6: enough (2^{128})
- **AI agents** must be signed
 - DNS CA
 - Address CA

Back to the beginning (the network of networks)



One single global Internet, plus each subset can still work in the extreme scenarios.

Impossible triangle



IPv6 for ...

Computers



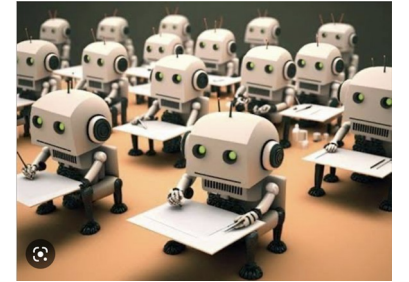
People



IoT



Robots



Uniqueness



We have to keep the distributed nature of the Internet and maintain the **UNIQUENESS** of the addresses/names/protocol parameters

RFC Considerations

- Security considerations
- IANA considerations
- Human-rights considerations
- AI considerations



Thanks!